вующие подходы не рассматривались в контексте использования ЛЦ для обнаружения атак направленного типа [5].

В связи с этим актуальной является задача выработки критериев применимости той или иной методики размещения ЛЦ для обнаружения атак направленного типа и проведения анализа существующих методик по этим критериям для выбора одной из них или обоснования необходимости разработки новой.

Помимо очевидных критериев, таких как простота реализации методики на практике и наличие количественного показателя эффективности размещения ложных целей, важно определить специальные критерии, на основании которых можно судить о применимости методики в условиях направленной атаки. Эти специальные критерии должны основываться на показателях, вытекающих из характерных свойств атак направленного типа. К таким свойствам относят [1,2]:

- наличие четко определенного объекта атаки;
- привлечение в случае необходимости значительных ресурсов для атаки;
- высокая квалификация атакующих и их осведомленность об атакуемом объекте;

Перечисленные особенности определяют многоступенчатость процесса направленной атаки. Нарушитель, осуществляющий направленную атаку, заинтересован в компрометации определенного подмножества узлов в сети. Эти узлы могут быть недоступны потенциальному нарушителю в начале атаки вследствие реализованной в сети политики разграничения доступа. Таким образом, для доступа к интересующим ресурсам злоумышленник может быть вынужден совершить ряд промежуточных атак на другие ресурсы сети, чтобы, используя их ресурсы, совершить атаку на интересующую цель.

Таким образом, методика размещения ложных целей в сети для обнаружения направленных атак должна учитывать тот факт, что в сети может быть реализована политика разграничения доступа. Другими словами, под размещением ложных систем подразумевается прежде всего распределение их по разным зонам межсетевого экрана.

С учетом этого, предлагается использовать следующий набор критериев для анализа применимости методик размещения ложных целей в сети для обнаружения направленных атак:

- простота реализации метода или алгоритма на практике;
- наличие количественного показателя эффективности размещения ложных целей;
- способность методики определять размещение ложных целей относительно границ зон межсетевого экрана с учетом правил разграничения доступа в сети.

Литература

1. Piggin R. Cyber security trends: What should keep CEOs awake at night //International Journal of Critical Infrastructure Protection. – 2016.

2. Sood, A.K., Enbody, R.J. Targeted Cyberattacks: A Superset of Advanced Persistent Threats // Security & Privacy, IEEE (Volume:11 , Issue: 1) . IEEE, 2013.

3. Медведовский И., Семьянов П., Леонов Д. Атака на Internet. – Litres, 2013.

4. Bringer M.L., Chelmecki, C.A., Fujinoki H A Survey: Recent Advances and Future Trends in Honeypot Research. // International Journal of Computer Network & Information Security. 2012. №4.

5. Алейнов Ю.В., Бондаренко В.В. Применение динамических систем пассивной регистрации сетевых атак для обеспечения безопасности компьютерных сетей // Сборник “Вычислительная техника и новые информационные технологии”. Уфа: УГАТУ, 2011. с. 126-131.

А.А. Бомм

РЕШЕНИЕ ЗАДАЧ БЕЗОПАСНОСТИ В ИГРОВОЙ ОБУЧАЮЩЕЙ СИСТЕМЕ «3DUCATION»

(Самарский национальный исследовательский университет
имени академика С.П. Королёва)

Развитие современных информационных технологий задает тенденцию разработки не только многофункциональных, но и безопасных приложений, которые способны выдержать конкуренцию на рынке информационных систем. Наряду с тривиальными задачами разработки вэб-приложений, остро стоят вопросы защиты от несанкционированного доступа и утечек данных. Защита информации (62%) и выполнение условий лицензионного соглашения (51%) являются основными причинами для защиты веб-приложений [1]. Одним из самых распространённых для получения несанкционированного доступа способов является использование уязвимостей систем аутентификации пользователей, в результате которых злоумышленники могут не только получить полный или частичный доступ к данным пользователя, но и вызвать сбои работы как отдельных узлов, так и системы в целом. Для решения задач безопасности необходимо полное понимание слабых мест в системе безопасности. Рассмотрению данных задач и посвящена данная работа.

Игровая обучающая система «3Ducation», разработанная на кафедре программных систем СГАУ, входит с информационное пространство школы информатики СГАУ наряду с сайтом Школы Информатики, сайтом дистанционного обучения и автоматизированной информационной системой (АИС) «Школа информатики СГАУ». Для удобства и комфорта конечного пользователя (доступ к различным системам должен осуществляться только через одну учетную запись) была разработана подсистема удаленной авторизации с использованием технологии единого входа (технология OpenID), которая позволяют клиенту перемещаться между различными разделами портала без повторной аутентификации [2].

Сама процедура аутентификации осуществляется через внутренний инструмент аутентификации, с момента запуска которого прецедентов взлома зафиксировано не было, что говорит о его надежности в контексте обеспечения безопасности. До настоящего времени персональные данные пользователя передавались на сервер в открытом виде, поэтому оставалась вероятность перехвата данных в момент аутентификации, например, если пользователь находился в одной беспроводной сети со злоумышленником.

Для решения задач безопасности системы «3Ducation» было решено использовать протокол шифрования SSL (англ. secure sockets layer), который позволяет шифровать данные на стороне сервера и клиента и в момент передачи обеспечивать их сохранность. Это является наиболее эффективным с точки зрения уровня обеспечения безопасности и затрат: в случае перехвата зашифрованных данных они уже не будут представлять для злоумышленника никакой ценности, так как расшифровка информации займет большое количество времени и средств.

С учетом того, что система «3Ducation» размещена на сервере СГАУ (virtual.itschool.ssau.ru), для ее защиты был использован сертификат класса 3, которым обладает СГАУ как юридическое лицо и который используется на всех поддоменах ssau.ru, это позволило избежать дополнительных издержек при обслуживании (оплата, предоставление необходимый данных и т.д.).

Для создания сертификата безопасности использовался инструмент OpenSSL, позволяющий создавать сертификат в формате *.pfx – представляющий из себя пару файлов из файла сертификата *.crt и файла закрытого ключа *.key. Установка сертификата безопасности производилась на веб-сервере IIS (англ. internet information services), работающем под управлением операционной системы Windows Server R2 2008.

После установки сертификата безопасности была проведена проверка корректности работы сервера: с помощью программы Wireshark был произведён перехват трафика во время аутентификации и работы клиента с игровой обучающей системой «3Ducation». Экспериментально было подтверждено, что информация, которой обменивается клиент и сервер, не представляет никакой ценности: без наличия закрытого ключа сертификата, хранящегося на сервере, расшифровка информации, в которой могут содержаться помимо технической информации: логин, пароль и другие личные данные, невозможна.

Таким образом, была реализована защита персональных данных пользователей системы «3Ducation» во время их передачи. В дальнейшем будут рассмотрены другие виды неявных угроз и целенаправленные виды атак с целью взлома и получения данных на стороне сервера. По результатам комплексного аудита безопасности системы планируется установка необходимых инструментов защиты, а также составление плана автоматического и запланированного аудита безопасности обучающей системы «3Ducation».

Литература

1. Как обеспечить безопасность веб-приложений? [Электронный ресурс]. – URL: http://internetno.net/category/obzoryi/mnenie/kak-obespechit-bezopasnost-veb-prilozhenijj/ (дата обращения 20.03.2016 г.).

2. Григорьев, А.О. Разработка пользовательского интерфейса виртуальной обучающей системы «3Ducation» [Текст]//Труды Всероссийской научно-технической конференции «Актуальные проблемы радиоэлектроники и телекоммуникаций». – Самара: изд-во СГАУ, 2014. – С. 145-148.

С.А. Бурлов

КОДИРОВАНИЕ С ПРОВЕРКОЙ НА ЧЕТНОСТЬ СВЕТОВОГО ПУЧКА ЛАГЕРРА-ГАУССА, НЕСУЩЕГО ОРБИТАЛЬНЫЙ УГЛОВОЙ МОМЕНТ

(Самарский национальный исследовательский университет
имени академика С.П. Королёва)

Введение. С конца XX века активно ведутся разработки квантового канала связи, использующего орбитальный угловой момент пучка фотонов для существенного повышения емкости канала связи. За разработками канала связи активно следуют разработки криптографических протоколов [2], [3]. По большей части они представляют собой модифицированную версию криптографического протокола *BB-84* с применением двух различных базисов: орбитально-углового, сформированного на состояниях мод с «чистым» показателем, и углового, описанного как суперпозиция определенного числа базовых состояний.

Работа [4] описывает Венский эксперимент по передаче сквозь сильно турбулентную атмосферу информации посредством суперпозиции световых пучков, противоположных по показателю орбитального углового момента. В эксперименте участвовала нейронная сеть, обеспечивающая детектирование сигнала, принимаемого на специальный экран. В процессе передачи информации неизбежно возникают искажения, которые приводят к ошибкам распознавания переданного значения.

Основной целью данной работы ставится рассмотрение возможности осуществления специального кодирования с проверкой на четность передаваемого сигнала для обеспечения информирования приемника о возможном искажении, полученном в процессе передачи.

Известно [1, 6], что пучки Лагерра-Гаусса можно получить из пучков Эрмита-Гаусса путем применения схемы, отраженной на рисунке 1. Пара цилиндрических линз переводит моду Эрмита-Гаусса с показателями (m, p) в моду Лагерра-Гаусса с показателями (m, p). На рисунке 2 отражены примеры профилей интенсивностей пучков Лагерра-Гаусса [5].